STATE of ARIZONA

Arizona **D**epartment **O**f **A**dministration	**Department** **STANDARD** **A800-M2-S03** **Rev 01**	**TITLE: <u>Vulnerability Scanning</u>** **Effective Date: DRAFT**

DRAFT

1. AUTHORITY

1.1. The authority for this standard is based on the ADOA Policy A800 – IT Security.

1.2. Authority flows from the Policies and Standards prepared by the Government Information Technology Agency (GITA) Standard P800-S830 paragraph 4.10.

2. PURPOSE

2.1. The purpose of this standard is to identify one component of a multi-layered protection strategy to secure ADOA's information and data from the risk of unauthorized access from external sources.

2.2. This standard recognizes ADOA Information Security's (AIS) use of a Vulnerability Scanning technology as the instrument for determining compliance to ADOA and Statewide IT Security Policy and Standards.

3. SCOPE

3.1. This policy applies to all ADOA Business Units, which includes divisions, contractors or other entities using departmental IT resources, information and data.

3.2. The ADOA Business Units, working in conjunction with the ADOA Information Security (AIS) Manager, are responsible for ensuring the effective implementation of ADOA Information Technology Security Policies, Standards, Guidelines and Procedures .

4. DEFINITIONS AND ABBREVIATIONS

4.1. Non Critical Vulnerability: A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source, but ***not** requiring timely response* to mitigate loss of data, damage to the system or severe impact to the business operation.

4.2. Critical Vulnerability: A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source *requiring timely response* to mitigate loss of data, damage to the system or severe impact to the business operation.

4.3. ADOA Security Assessment Team: ADOA personnel who will participate in the assessment and provide assistance in performing the assessment information gathering and testing.

5. STANDARD

This standard establishes one of the minimum components for protecting ADOA's IT Resources. Multi-layered protection will be employed at the Internet gateway, the network server, and the desktop levels to prevent introduction of malicious code or unauthorized access into ADOA's information systems.

5.1. **Network and Host Vulnerability Scanners:** will be used to test for the vulnerabilities of internal systems and network perimeter defenses. Scanning for vulnerability is one component of ADOA's comprehensive network security solutions. This component allows security administrators to measure security, manage risk and eliminate vulnerabilities, providing a more secure network environment.

A. Vulnerability scanners will have the ability to:

1. Map the network or inventory systems and services on ADOA's network.
2. Identify security gaps by confirming vulnerabilities.
3. Provide effective analysis of vulnerability data.
4. Provide comprehensive reports and charts for effective decision making.
5. Define and enforce valid security policies when used during security device installation and certification.

5.2. **Frequency of Scanning:**
Review of the security controls in each system will be performed when significant modifications are made to the system (when put into production) or at least every 30 days to assure that management, operational and technical controls are functioning effectively. Penetration testing of the network and host devices will be performed annually. The scope and frequency of the review should coincide with the acceptable level of risk for the system.

A. **Network Scanning**: every 30 days using Nessus

B. **Host Scanning:** every 30 days using Nessus

C. **Penetration Testing:** annually Nessus and available tools

D. **Firewall Service Module/IDSM:** monitoring continuously

E. **Client Firewall:** monitoring continuously

5.3. **An independent review:** will be performed at least every three years for the security controls for the ADOA network infrastructure host systems and each major application.

DRAFT

5.4. **Reporting of Identified Vulnerabilities:**

A. **Critical Vulnerability Report** shall be produced to identify any critical vulnerabilities (as defined in Definitions) discovered as a result of the vulnerability or penetration tests. The report shall be delivered by the ADOA Information Security Manager *within two business days* of completion of the vulnerability test, to the appropriate ADOA Business Unit to make the required corrections to mitigate risk of the vulnerabilities noted.

B. **Non-Critical Vulnerability Report** shall be produced to identify any non-critical vulnerabilities (as defined in Definitions) discovered as a result of the vulnerability or penetration tests (a summary of all vulnerabilities will be provided, to include critical vulnerabilities. The report shall be delivered by the ADOA Information Security Manager *five business days* of completion of the vulnerability test, to the appropriate ADOA Business Unit to make the required corrections to mitigate risk of the vulnerabilities noted.

C. **The Final Vulnerability Report** shall:

1. Ensure each vulnerability be identified by device (by IP address)
2. Ensure each vulnerability be identified by location and the nature of the vulnerability.
3. Have the methodology used to determine that the vulnerability described.
4. Explain the nature, and impact to ADOA security.
5. Include detailed recommendations that ADOA should take to alleviate the risk and vulnerability in a timely manner.

5.5. **Tests performed:** Perform vulnerability assessment and penetration test on approximately 30 subnets, one (1) class "B" IP range (with approximately 1000 IP addresses total) on 20 VLANS from:

A. The Internet
B. Designated interface external to the ADOA firewalls, but within the Arizona State infrastructure
C. All interfaces internal to the ADOA network

5.6. **Follow-up Procedures to Correct Identified Vulnerabilities:** the following items will be included in a report for each vulnerability scan and penetration test:

A. Overview of methodology for assessing network vulnerability
B. Description of the methodology used to identify critical, non-critical, and informational issues.
C. Findings and overview of health and security of network

DRAFT

D. Critical vulnerabilities found during assessment and an analysis of impact on network health and security.
E. Remediation recommendations for critical vulnerabilities and steps needed to meet the required standards
F. Non-critical vulnerabilities found during assessment and an analysis of impact on network health and security.
G. Remediation recommendations for non-critical vulnerabilities and steps needed to meet the required standards.
H. Recommended baseline for annual assessment of network vulnerability to exploitation incidents
I. Recommended changes and improvements to be made to current ADOA policies and standards to reflect adherence to industry standards

DRAFT

6. STANDARD NON-COMPLIANCE

See ADOA Policy – A800 IT Security, paragraph 7. Policy Non-Compliance Statement

7. REFERENCES

7.1. ADOA Department Policy – A800, IT Security
7.2. Statewide Policy – P800, IT Security

8. ATTACHMENTS

8.1. No attachments accompany this standard.